DNS Tunneling Misuses

Prashant Jeet Singh[1] Virendra Kumar[2] Sanchita Mishra[3] Shilpi Srivastava[4] Santosh Kumar Upadhyay[5]

[1,2,3,4]Graduate Student [5]Assistant Professor

[1,2,3,4,5]Department of Computer Science and Engineering

[1,2,4,5]Galgotias College of Engineering and Technology, Greater Noida, India [3]Invertis University, Bareilly, India

Abstract— DNS, Domain Name System, is one of the foundational protocols for Internet to work. It resolves hostnames to scientific disciplined addresses known as IP addresses which enables applications such as web browsers and humans to use internet or other networks easily. Because of its limited functionality, it is wide open in many enterprise firewalls with a very less attention from enterprise security monitoring. Due to all these factors, many tools have evolved to set up covert information tunneling channels through DNS which goes undetected causing significant information exfiltration risks to organizations and financial losses to ISPs. Hence, it's vital to investigate and prevent DNS tunneling. In this paper we walk through DNS overview, different DNS tunneling tools and techniques to block it.

Key words: DNS Tunneling, IP addresses, hostnames, firewalls

I. INTRODUCTION

Web browsing, emails and online social networking have become a vital part of end users and organizations. The job of DNS is to allow application and users to function using domain names instead of IP addresses which are hard to remember and maintain. However many tools have been developed to carry information other than name resolution through DNS. This technique is commonly known as DNS tunneling. A common motivation for users to use thiskind of application is to get free internet via open Wi-Fi points such as Airports and Cafe where DNS traffic is allowed without any charges. In many countries, ISPs (Internet service providers) do not charge there users for DNS traffic, hence allowing people to use DNS Tunnel applications for free internet over 2G, 3G and 4G networks. Many organizations also allow DNS traffic unfiltered and unmonitored at their enterprise firewalls.

Thus, DNS tunneling can pose a significant risk of information leakage as it can bypass all the data prevention solutions such DLP (Data Loss Prevention), enterprise web proxies and other security solutions.

II. DNS OVERVIEW

The Domain Name System (DNS) implements the functionality of translating and locating hostnames to their respective IP addresses. DNS functionality becomes a necessary requirement when an application or a human tries to communicate with a remote system from a local computer, the source is likely to only know the host name of the remote service/system, however TCP/IP protocol suite functions using IP addresses not the hostnames. So DNS provides a mechanism to do mapping between hostnames and IP address using a distributed hierarchical database of system/service names and IP addresses. A source looking for IP address of any remote system or service is known as DNS Client.

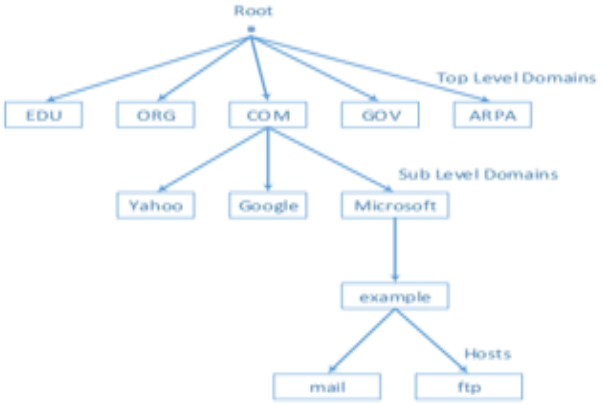

Fig. 1: Domain Name System Hierarchal Arrangement

We can say that DNS database is similar to local hosts file (/etc/hosts or C:\Windows\system32\drivers\etc\hosts)which were primarily used to maintain similar mapping between names and IP addresses on a local computer in the beginning of Internet age.

DNS server, also known as Name Server, when receives a request from DNS client, looks for the hostname within the request and tries to resolve it to an IP address.It then returns the found IP to DNS Client, which uses the IP to communicate directly with target system.

Fig. 2: DNS Query

A. *Authoritative Vs Recursive Name Queries*

DNS Queries, name lookup requests from DNS clients, are generally categorized under Authoritative or Recursive Queries. An authoritative queries is the one for which the requested DNS server maintains the mapping information locally and is parent for this information. On the other hand, the queries for which the requested DNS does not have any information locally instead it searches for the same with the help of other DNS servers are known as Recursive queries. Following diagram illustrates how a recursive query is completed:

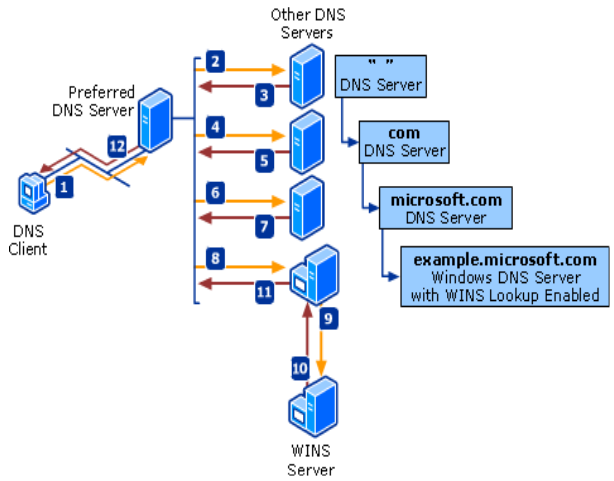

Fig. 3: Recursive DNS Query

B. Authoritative Vs Caching Name Servers

DNS servers are basically divided into two major categories i.e. Authoritative and Caching. As mentioned earlier, the servers maintaining (as parent) the information about a specific domain are known as Authoritative Name Server for that domain. However, when a name server fetches information from another server during a recursive name query and stores this information locally for some duration in order to serve other DNS clients looking for same information is known as Caching DNS server. This functionality enables DNS servers to reply faster as the information is now locally cached.

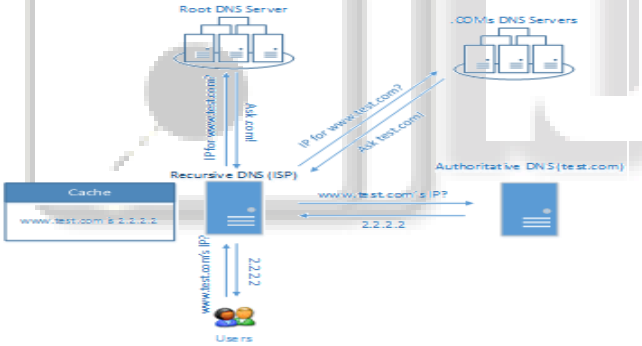

Fig. 4: Caching DNS Servers

C. DNS Records

DNS entries for mapping the different types of information are known as DNS records. There are little more than 30 types of DNS records, few of them are:

- A record: maps hostname to IPv4 address
- AAAA record: maps hostname to IPv6 address
- MX record: info about Mail Server of a domain
- TXT record: Any text data
- NULL record: Experimental record type

III. DNS TUNNEL

DNS is a very critical service for any organization to function over computer networks. Due to its wide presence but limited functionality, it is often ignored by the security monitoring teams, making it a very convenient target for attackers to misuse. One of the several ways DNS can be misused is DNS Tunneling. It is basically a technique to hide data within DNS requests for different records. Now days, it has been frequently used to facilitate the following:

- Command and control communication for malwares (botnets)
- Data exfiltration from enterprises without detection
- Exploiting WiFi at public places such as airports
- Exploiting ISP networks for free internet usage

Many tools/applications have evolved over time to facilitate DNS tunneling using computers or Mobile phones. Many of these tools are available freely within Google Play store for mobile users. Some of them are:

For Mobile (Android):

- Your Freedom
- Iodine
- Tunnel Guru – Slow DNS

For Computers (Windows/Linux/Mac):

- Heyoka
- Your Freedom
- Iodine
- DNScat

The tunnel involves a client application such as mentioned above and a specially crafted DNS server. The client application is well designed to hide any kind of data such as Web, Mail, and Social Networking within DNS requests, generally requests for TXT or Null records, for a specific domain, thus redirecting all queries to their specially crafted DNS server, which processes the information hidden in these packets. The responses are also sent hidden within standard DNS responses.Following diagram illustrates DNS Tunnel workflow for an established connection.

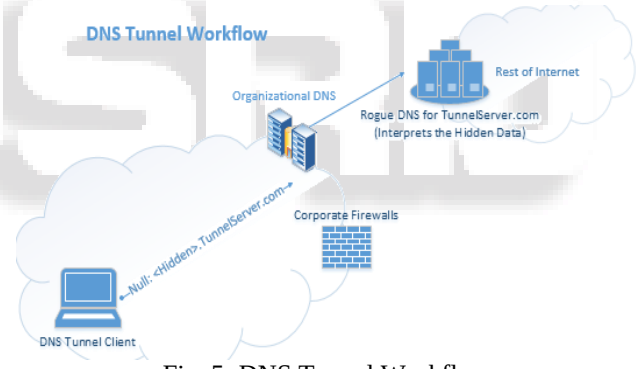

Fig. 5: DNS Tunnel Workflow

A sample NULL query and response involved in DNS tunnel looks like below:

DNS
Query:aD.DP4cJvOeXMaHheVAofamJT
jyutD8RZ06XKURtgtO.s28.1yf.de

DNS Server
Response:bM.UkyqLH2sNkIDy0XIYapj
5xnEyVVIx6ixFVViPfk6RxUnkL7zakC40
WPjE0NLbYu.SIwHGnCg7rZlri6qbnp2L
rZssWIBdU5HIJ4VmGsvbWAwjR81t6Ft
ZIIpKYEH.s28.1yf.de

In case, where users try to exploit public WiFi spots or ISP 2G/3G networks for free internet, generally exploit the fact that DNS communication is allowed free of cost on these networks. A very good example is at airports where the WiFi service prompts for specific amount of fee

to allow browsing. However that can be easily bypassed with the use if DNS tunnel.

This way DNS tunnel not only imposes financial losses to ISP and WiFi service providers but also facilitates stealing of digital data from organization without being detected as many organizations ignore monitoring of DNS traffic.

IV. DETECTION AND PREVENTION

Detecting and preventing DNS tunnel is a challenge in its own due to the variety of Tunnel application using many different algorithms to generate and encapsulate traffic within DNS packets. Due to this, creation of single detection signatures in DPI (Deep Packet Inspection) solutions does not mitigate it. However, following methods can be used to mitigate DNS tunneling:

1) Blocking traffic for known DNS Tunnel or malicious domains: Organizations should have a source, such as Infoblox RPZ, to get feeds about known malicious or DNS Tunnel domains. Also the DNS server should be configured to block queries based on these trusted feeds.
2) Restricting the amount of free DNS traffic per client for a specific time period: Based on the category or choice of users, organizations should benchmark the amount of traffic being utilized by a single user within a given period of time. Rules should be created to generate alerts and block when users cross their quota.
3) Restriction on free DNS traffic: ISP (Internet Service Providers) and WiFi providers such as Airports should not allow free DNS traffic targeted other than the providers DNS. This will enable the providers to control the free traffic passing through their DNS servers.
4) Whitelisting in NULL records: On the basis of feasibility, all NULL queries should be blocked. However certain legitimate application also use NULL queries to exchange data, this should be identified and whitelisted.
5) Size of DNS Queries: Generally the size of the queries involved in DNS Tunneling misuses ishaving hostname bigger than 52 characters. All such traffic should be actively monitored and blocked if required.
6) Deep Packet Inspection for DNS: DPI solutions supporting DNS protocols should be implemented to inspect DNS UDP traffic for a better visibility.

V. CONCLUSION

The purpose of this document is to show how DNS Tunneling is being frequently used worldwide, especially in developing countries, to hamper businesses financially or to steal sensitive digital data. These DNS abuses are enormously growing and without proper technology controls to protect networks, the businesses and ISPs could be highly impacted.

REFERENCES

[1] Liang Zhu, Zi Hu, John Heidemann, Duane Wessels, Allison Mankin and Nikita Somaiya, "Connection-Oriented DNS to Improve Privacy and Security", IEEE, 2015.
[2] Naveen Kumar and Kamal Kumar Ranga "A Framework for Using Cryptography for DNS Security",IJCSMCVol. 4, 6, June 2015.
[3] Nobuhiro Shibata, Yasuo Musashi, Dennis Arturo Ludena Romana, Shinichiro Kubota and Kenichi Sugitani, "Trends in Host Search Attack in DNS Query Request Packet Traffic", Fifth International Conference on Intelligent Networks and Intelligent Systems, 2012.
[4] Samuel Marchal, J´erˆome Franc¸ois, Cynthia Wagner, Radu State and Alexandre Dulaunoy, Thomas Engel and Olivier Festor, "DNSSM: A Large Scale Passive DNS Security Monitoring Framework", IEEE Network Operations and Management Symposium (NOMS): Mini-Conference, 2012.
[5] Naveen Kumar Tiwari and Sanjay Khakhil, "Security System for DNS using Cryptography",International Journal of Computer Application(0975 – 8887) Volume 120 – No., 17, June 2011.
[6] L. Bilge, E. Kirda, C. Kruegel and M. Balduzzi, "Finding malicious domains using passive dns analysis", NDSS'11, 18th Annual Network & Distributed System Security Symposium, 6-9 February 2011, San Diego, California, USA, February 2011.
[7] B. Zdrnja, "Security monitoring of dns traffic", May 2006.
[8] SANS Institute InfoSec Reading Room, "Detecting DNS Tunneling",https://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152.

